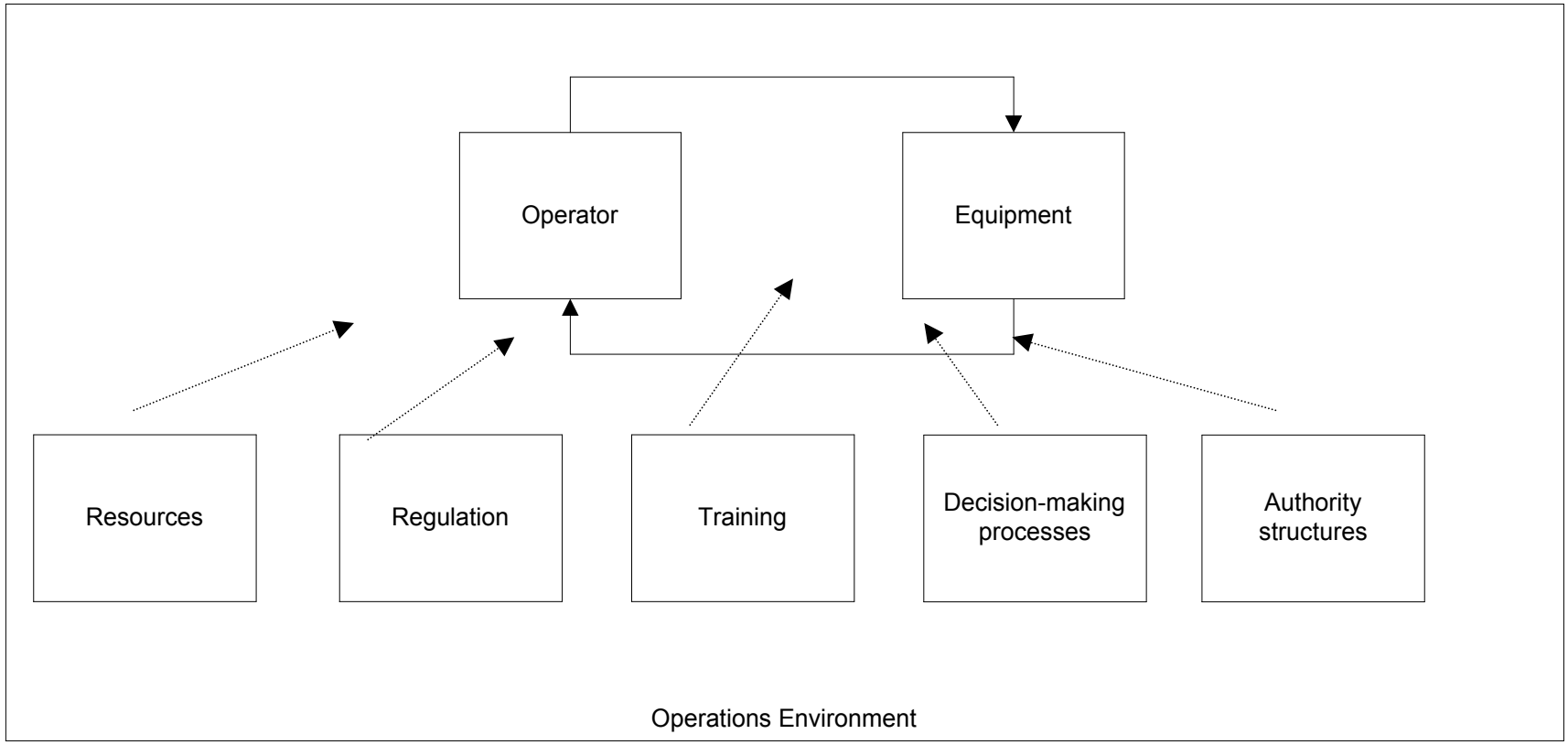
Safety, Reliability, Stewardship, and Regret: Contributions to Dependable System Design from the Study of Highly Reliable Organizations

Andrew Koehler, PhD
Statistical Sciences, D-1
Los Alamos National Laboratory

LA-UR-05-8477

System dependability: the role of organizational theory



Organizations matter—how do we craft social structures that promote dependable system traits?

- Social organizations cannot be engineered as easily as technical systems
- Interactions between the system and the organization that designs/operates it are dynamic, complex, and partly a result of history
- There are examples of organizations with great success at operation of technical systems. There are also examples of organizational forms which are not compatible with system dependability
- How can dependable system organizational “traits” be encouraged?

An observation of an anomaly:

How is it that some organizations are able to operate inherently hazardous technical systems with more success than is suggested by the inherent characteristics of the technology?

- USN Carrier Aviation
- Nuclear Power Plants
- Strategic Air Command
- Commercial Aviation/Air Traffic Control
- Maritime Systems
- etc.

A framework

Social Benefit-Cost of Activity $= \sum_{t}((B_t - \sum_{i,j}(X_{it}P_{it} + X_{jt}P_{jt}))$

where

B_t is the collection of social benefits per unit of time produced by the technical activity

X_i, X_j are specific per time unit hazards from equipment and anthropogenic errors

P_i, P_j are specific per time probabilities of hazard occurrence from equipment and anthropogenic error

However :

P_i, P_j, X_i, X_j are non-independent results of common factor operator organizational actions/characteristics

B_t, X_i, X_j are functions of common factors external to the organization such as public dread, trust/confidence

High Reliability Organization Theory—a long term research program in the social sciences

HRO and Dependability:

1) the interconnected non-isolatable nature of social and equipment roles in creating risks,
2) that risks (from whatever source) are dynamic and partially controllable through on-going vigilance
3) that HRO technical activities function within a framework of a social relationship which can be harmed by operational failure

HRO Organization: Internal Traits

Defined by:

1) Strong sense of mission
2) Public commitments by high-status leaders
3) Culture of reliability, w/norms of equal value of reliable production and safety
4) Structural flexibility and redundancy
5) Collegial, de-centralized authority patterns in the face of high tempo operations
6) Flexible decision-making processes involving operating teams
7) Process enabling continual search for improvement
8) Processes that reward the discovery & reporting of error, even one's own
9) Process of review and discovery that includes stakeholders

To which the demands of long term stewardship (supporting the development of public trust and confidence (PT&C) and institutional constancy (C)or both) add the following necessary traits:

1) Institutional norms that nurture commitments across many generations (C)
2) High managerial competence and discipline in meeting realistic schedules (PT&C)
3) Pursue technical options clearly demonstrated to broad segments of the public (PT&C)
4) Self assessment to "get ahead of problems before discovery by outsiders" (PT&C)
5) Institutionalized responsibility and resources to protect Stewardship related activities throughout the organization
6) Resources for "transferring requisite technical/institutional knowledge across from one work/management generation to the next (C)
7) Analytical and resource support for "future impact analysis" (C)
8) Capacity to detect/remedy the early onset of likely failure that threatens the future, and assurance of redemption if failures occur (C)

Technology: Desirable Traits Associated with HRO Performance

Defined by:
1) Maintained surplus (resources, capacity)
2) Managed coupling (introduction of friction where necessary)
3) Flexibility and decomposibility
4) Data provision that supports operator vigilance
5) Graceful failure
6) Resilience

Traits of External Relationships Supporting HRO Organizational Performance

1) Strong superordinate institutional visibility within parent organization
2) Strong presence of stake-holding groups (watchers)

To which the demands of long term stewardship (supporting the development of public trust and confidence (PT&C) and institutional constancy (C)or both) add the following necessary traits:

1) Mechanisms for boundary spanning processes between the unit & "watchers" (PT&C)
2) Venues for credible, current operational information available on a timely basis (PT&C)
3) Early, continuous, involvement of stake holders advisory groups w/freq. contact, candor & rapid, full response (PT&C)
4) Timely carrying out of agreements unless modified through an open process established in advance (PT&C)
5) Active, periodic presence of very high agency leaders, visible and accessible to citizens at important agency field sites (PT&C)
6) Unmistakable agency/program residential presence locally that contributes to community affairs and pays its fair share of the tax burden (PT&C)
7) Negotiated benefits to the community with the resources that might be needed to detect and respond to unexpected costs [imposed by the activity] (PT&C)

Traits of External Relationships Allowing HRO Organizational Performance

1) Predictability/adequacy of resources, support
2) Necessary degree (determined by system technology characteristics) of deference to technical expertise of system operators
3) Public acceptance of costs, trust in organization as a "good steward"
4) Public constancy of need for benefits produced by the system
5) Support for system watching efforts

Towards Organizational Design to Promote Dependability Traits

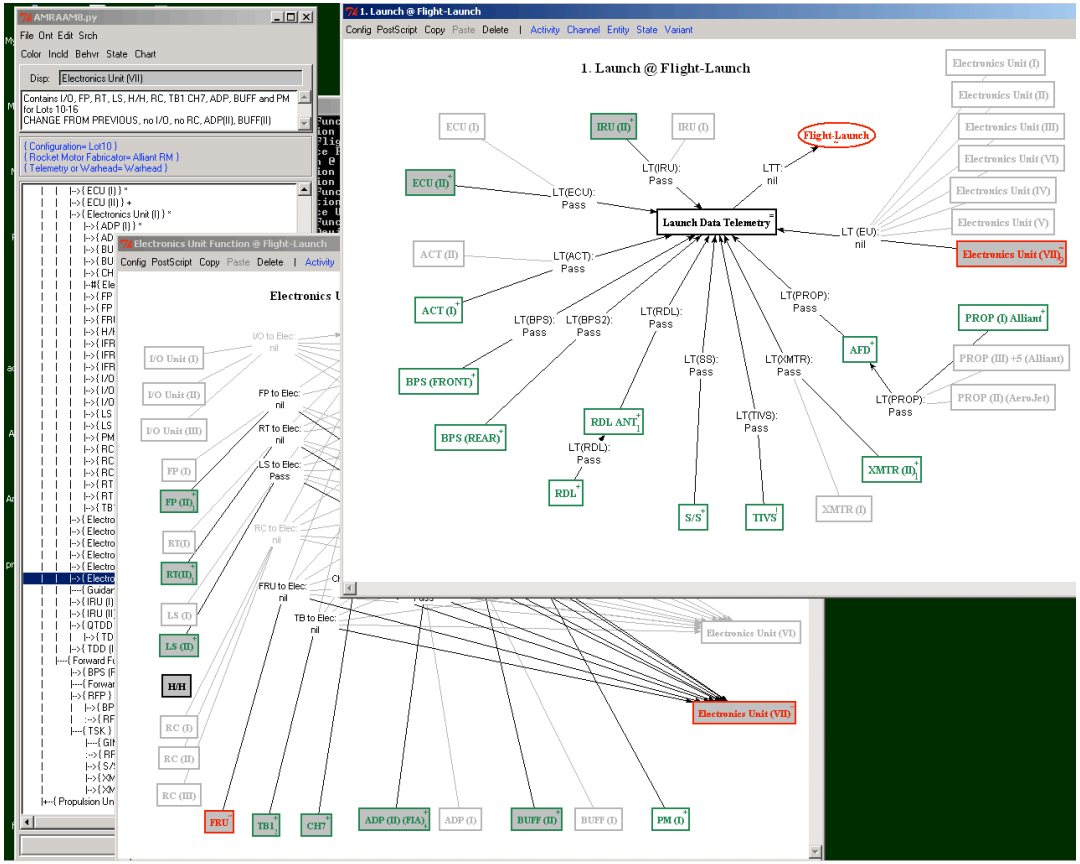
1) Promotion of focused case studies—how to we connect social and technical factors together

   Explaining how analog systems perform in different operational environments and how can we “predict” what will happen

2) Recursive system performance simulation

   Explain linkages between quantifiable “organizational” factors (budgets, maintenance practices, operational patterns) and system technical characteristics

Some progress towards these goals



A number of capabilities and tools are starting to emerge that could be useful in meeting these cross disciplinary goals—Bayesian analysis tools, system analysis, agent based modeling methods, qualitative methods.

The real question is on both within the engineering and social science communities is there the discipline needed to study organizational-technical links as part of achieving system dependability